TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

Validators Performance Efficiency Consensus (VPEC): A Public Blockchain

[1]Islahuddin Jalal, [2]Zarina Shukur and [3]Khairul Azmi Bin Abu Bakar

[1,2,3]Faculty of Science and Information Technology, UniversitiKebangsaan Malaysian, Malaysia
[1]Faculty of Computer Education and Information Technology, Kabul Educaiton University, Afghanistan
islahuddinjalal@yahoo.com[1]; zarinashukur@ukm.edu.my[2], khairul.azmi@ukm.edu.my[3]

Article Info
Volume 83
Page Number: 17530 - 17539
Publication Issue:
May - June 2020

Article History
Article Received*: 1May 2020*
Revised*: 11 May 2020*
Accepted*: 20 May 2020*
Publication*: 24May 2020*

Abstract

The consensus is a problem in the distributed system. There are different nodes in the distributed system, and these nodes agree on specific criteria. As we know that there is no central authority in the distributed system, to control and manage. Therefore, block-chain is also a distributed system. The consensus is the core part of it. For the block-chain system, several consensus algorithms are designed. They have different philosophy behind since bitcoin appearance. Some of the consensus algorithms consume more energy, having low or high throughput, and low latency. In this article, we proposed a novel consensus algorithm for the block-chain system. It is more efficient and provided fairness to ordinary users. The fairness is, in terms of getting the reward for the creation of a new block in the block-chain system.

Keywords; *Blockchain Consensus, Consensus Algorithm, Consensus Mechanism*

I. INTRODUCTION

The development of consensus algorithms has been around for more than 40 years (Muratov, Lebedev, Iushkevich, Nasrulin, & Takemiya, 2018). It is not only used in distributed system but it is also used in health for controlling weight of human (Siew Pheng Chan, William C. Chui, Kwok Wing Lro, Kuo Chin Huang, Normita D. Leyesa, Wen Yuan Lin, Roberto C. Mirasol, Yolanda R. Robles, Beng Hea Tey, 2012). It becomes more popular with the advent of block-chain technology. Blockchain is welcomed by many people around the world (Kamal, Saad, Kok, & Hussain, 2018). It increases the privacy and reliability provided to critical and sensitive transactions (Safavi, Meer, Keneth Joel Melanie, & Shukur, 2019) by using encryption algorithms such as symmetric algorithm (i.e. AES) or asymmetric algorithms (i.e RSA, ECDH etc.) on the peer to peer network (Nur Husna Azizul, Abdullah Mohd Zin, Ravie Chandren Muniyandi, 2019). Blockchain is the underlying technology of the bitcoin. Bitcoin is created against financial crises (King, 2019) to replace digital cash like e-money which is used in different countries like (Husnil Khatimah, 2019). The basic idea of the block-chain is to eliminate centralization, where some unknown parties lack consensus in the environment to maintain and manage transactions or any other activities in them. The mechanism by which many nodes agree with each other is called a consensus protocol. Consensus protocol is not a single strategy or algorithm which suits all block-chains' platforms, and different types of algorithms are available, including PoW(Satoshi, 2009), PoS(Chohan, 2018), PoL(Milutinovic, He, Wu, & Kanwal, 2016), PoV(Li, Li, Hou, Li, & Chen, 2018), Tendermint(Kwon, 2014), PoC(Xue et al., 2018), DPoS(Snider, Samani, & Jain, 2018), PBFT (De Angelis et al., 2018), YAC-BFT (Muratov et al., 2018), Raft (Lamport et al., 2014), PoET, SCP (Mizoguchi & Lippard, 1998), Ripple (Schwartz, Youngs, & Britto, 2014), Hashgraph(Baird, 2018),

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

Helix (Asayag et al., 2018) and HoneyBadgerBFT(Miller, Xia, Croman, Shi, & Song, 2016) etc. with some of their unique characteristics. These consensus algorithms are designed with different concepts behind, such as scalability, liveness, safety, latency, energy consumption, fault tolerance, throughput issues and more. Some consensus algorithms like (Asayag et al., 2018), (Miller et al., 2016) and (Baird, 2018) cover the order of transactions, the choice of leaders, and transaction selection for block but lacking the fairness in mining strategy for ordinary users in the permissionless block-chain system. Take a look at the mining strategies of the two most popular consensus algorithms such as PoW and PoS.

In this paper, we have proposed a new consensus algorithm for block-chain's system. It brings fairness to the block chain system, in terms of earning rewards for the creation of new blocks. The proposed consensus algorithm ensures safety, fairness, liveness, scalability, and low consumption power in the block-chain system. The rest of the paper is described in the following sections. Section 2 is related work. Section 3 addresses the issues of PoW and PoS consensus algorithms. Section 4 summarizes the core part of this paper, which is a novel consensus mechanism (VPEC). In Section 5, VPEC is evaluated and analyzed. Various consensus algorithms against VPEC is discussed in section 6, To summarize this article, and future directions are provided in Section 7.

II. RELATED WORK

2.1. Proof-of-Work (PoW)

PoW(Satoshi, 2009) is designed for Bitcoin's block-chain. The consensus is done in the Bitcoin system by broadcasting transactions to all the nodes in the system. Each node of the block-chain system receives the new transactions and add them into a block. This process is complicated, and it needs a high-performance computing resources like Application Specific Integrated Circuit (ASIC) or Graphics Processing Units (GPU). The miner does not know the number of iterations to find the required hash value, but it is effortless to verify the process. When a node finds the needed value of a Proof-of-Work, it broadcasts the block to all the nodes in the block-chain system. The other nodes accept the block only if all transactions in it are valid and not already spent. Once approved, each node appends the block with the last agreed blocks by using the previous hash value, as a result producing a chain of blocks that is called the block-chain. The block-chain functions are like a transaction ledger, and together with the mining process, Nakamoto'sBitcoin protocol solves the critical double-spending problem in cryptocurrency in the absence of a central authority, with the assumption that honest nodes control the majority of the CPU power in the Bitcoin network. The honest nodes are not cooperating with malicious nodes to attack the system. There is also a chance of finding the hash value at the same time by more than one miner, and such a situation is called a fork. As such, the longest block-chain represents the consensus of transaction history (Reis, Amorim, Melao, & Matos, 2016).

The winner gets a reward of 12.5 bitcoins, and it is reduced to half every four years. In the PoW consensus, there is also a chance of 51% attacks where the mining pool controls 51% of mining power. Though, the mining pool is valuable to gather a large amount of computing power but unfair to the new node to join alone and get the mining reward. Because the new node or individual does not have that much computing power as the mining pool has (Reis et al., 2016). According to (Yli-huumo, Ko, Choi, Park, & Smolander, 2016), the estimated operating cost of the bitcoin network that uses the PoW as a consensus algorithm is 23.88 billion Euro for four and a half year. This is 45% more than the real price of the bitcoin.

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

2.2. Proof-of-Stake (PoS)

Proof-of-Stake is designed as an alternative consensus algorithm to PoW, which is the resource wasting, Concentration of hash power and slow speed of transactions (Mingxiao, Xiaofeng, Zhe, Xiangwei, & Qijun, 2017). In this, the miner should have a stake which is approximately equal to 2000 USD. The PoS algorithms randomly select miner for block creation, and no miner can predict its turn in advance. The miners produce a block and added to the block-chain. The miner will be rewarded, and if it fails to add a block in the block-chain, then the miner will be fined as much as the reward. The mining depends on the amount of stake a person has in the system. If a miner has more stake in the block-chain, the chances of mining are more. For instance, If the stake in the given crypto-currency is at 1%, you can mint up-to 1% of the transactions (Jain, Arora, Shukla, Patil, & Sawant-patil, 2018).

Three limitations of Proof of Work (PoW) and Proof of Stake (PoS) pointed out by (Mingxiao et al., 2017) which are as follow:

I. Waste of resources

Nodes with high hashing capabilities can receive the corresponding bitcoin as a reward. This is the main way to get Bitcoin, which forces people to upgrade their hardware. Participants need to spend a lot of money to purchase a special mining machine, and the machine consumes a lot of power during the calculation process.

II. The slow speed of transactions

In order to reduce the generation of single block or branch of the chain, the computation time of each block cannot be too short. The average calculation time for this block is 10 minutes. But not sure about the time interval between the two blocks. The largest interval in history is more than one hour, and the minimum interval is less than one second. This time there are significant limitations in the application of instant payment.

III. The concentration of hashing power

As the difficulty of mining increases, it is difficult for one to solve mathematical puzzles. In order to solve this puzzle, some organizations have established “mining pools”, and miners in the pool have solved mathematical puzzles together. After solving the mathematical puzzle and getting Bitcoin as a reward, the miners allocated Bitcoin based on their contributions. However, due to the existence of mining pools, global hashing capabilities have become concentrated. If a pool or some combination pools have a hashing capacity of more than 50%, they are easy to have a monopoly in accounting. At present, the hash capacity of the world's top six mining pools has exceeded 50% of the global hash capacity.

III. ISSUES OF POW AND POS CONSENSUS ALGORITHMS

A summary of the problems of different consensus algorithms is shown below in Table 1.

Table 1: Consensus Algorithms with Available Issues

Consensus Algorithms	Available issues
PoW	Energy and Computation Expenditure, Uselessness computation, 51% attack, Forking, Un-fairness
PoS	Minting dependency on stake, Forking, Nothing-at-stake, Un-fairness

3.1 Energy and computation expenditure

The difficulty level in the PoW keeps increasing in the block-chain. Therefore, more power and dedicated hardware (such as an ASIC) are needed to resolve the hash value, having a specific number of zero in front, which increases the costs of finding the hash value. The cost of finding a hash value is difficult to control. Mining can only be used for

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

mining pools with expensive hardware that leads to system centralization.

3.2 Uselessness of Computation

All miners are competing for competition to create new blocks. They are competing to find a specific hash value. The hash value can be calculated from an unknown number of iterations. Therefore, they consume more energy. As a result, one of them succeeded, the hard work of other miners became useless, and their hard work could not be applied anywhere else.

3.3 Forking

Due to the greediness of miners, forks are available in consensus algorithms such as PoW and PoS. They are competing for a new block creation award. Therefore, it causes the blockchain to split into two parts.

3.4 51% Attack

This attack occurs when the group of miners controls more than 50% of the computing power of finding the difficulty value in the PoW system. This attack causes to create the issues such as double spending and ignoring specific user's transactions in block-chain(Yli-huumo et al., 2016).

3.5 Un-fairness

The PoW and PoS make it very difficult for the poor people who wish to join the block-chain as a miner. Due to the cost of using expensive technology such as ASIC (PoW) and holding stake (PoS).

3.6 Minting dependency on stake.

The minting depends on the amount of stake a person has in the system. If a minter has held a high stake, the chances of minting are more as is discussed in (Sankar et al., 2017). If the stake in the given cryptocurrency is at 1%, the person can mint up-to 1% of the transactions.

3.7 Nothing-at-stake

There is no penalty defined for participants of double spending attack and contributing to multiple block-chain forks in the PoS consensus algorithm.

IV. VALIDATOR'S PERFORMANCE EFFICIENCY CONSENSUS (VPEC) ALGORITHM

VPEC consensus mechanism is designed for public block-chain. It can also be modified for consortium block-chain as well. It provides fairness among the miners in terms of incentives. In VPEC, every active miner shows its performance by validating and verifying the number of transactions in the block. As it is opposite to, solving a complex puzzle, which is the finding of a hash value with a specified number of zeros in front of the hash code. Finding hash values is time consuming, and the heat emitted by the technology used can affect the environment and consume a lot of energy. As a result, the process of solving the mathematical puzzle becomes very expensive. In this process, when time reaches to create a new block which is every ten minutes. There should be a pseudo-randomly lottery among all the active miners. An overview of the VPEC mechanism is shown in figure 1.

The criteria for selecting a lucky draw verifiers based on the performance of the last ten minutes are as follows:

- Active miners become active for the last ten minutesMaximum transactions validated and verified by miners will be selected for the lucky draw.

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

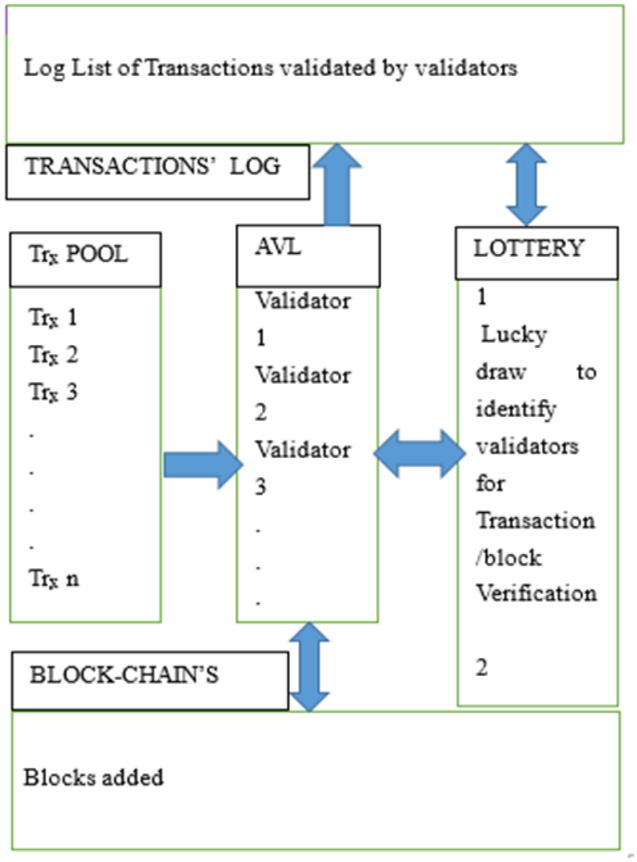

Figure 1.Overview diagram of VPEC mechanism.

4.1 VPEC Transaction Pool

The user sends the transaction to the transaction pool. The miner will pull a transaction from the transaction pool for further processing. The pool will not include similar transactions from the same user.

4.2 VPEC Lottery Section

The lottery section includes two sections; First, lucky draw to determines the verifier for Transaction/block verification. Second, the lucky draw is used to motivate the miners for incentivizing the creator of a new block of the block-chain. The first section of the lottery will choose 51% of validators from the active validator list (AVL). The draw will be made in all the active validators in AVL. The second section of the lottery executes when time reaches to create a new block, which is every ten minutes. There should be a pseudo-random lucky draw between all active validators in AVL. The overview of the lottery section is show in the following Figure 3. The criteria of selection for the lottery is based on the performance in terms of validations, and verification of valid transactions are high. Performance can be checked from the transaction log section in the last 90 minutes by the lottery section. During this process, the number of transactions is validated or verified by each candidate are shown. The lucky draw rules for the second part of the lottery section are as follows:

- Top Ten list validators are selected for the lottery
- Pseudo-randomly lottery is done in every 10 minutes.
- If one wins the lottery from the chosen list, then it will be out of the list
- Will not be included in the lottery until all the validators in the list win lottery
- The winner will wait up to the last miner is selected of the list by the lottery section
- For the next lucky draw, it is not necessary that the same list will be selected, the selection is based on its performance of validating/verifying transactions in the block.
- The winner of every lucky draw will be allowed to create a block, and reward will be awarded.

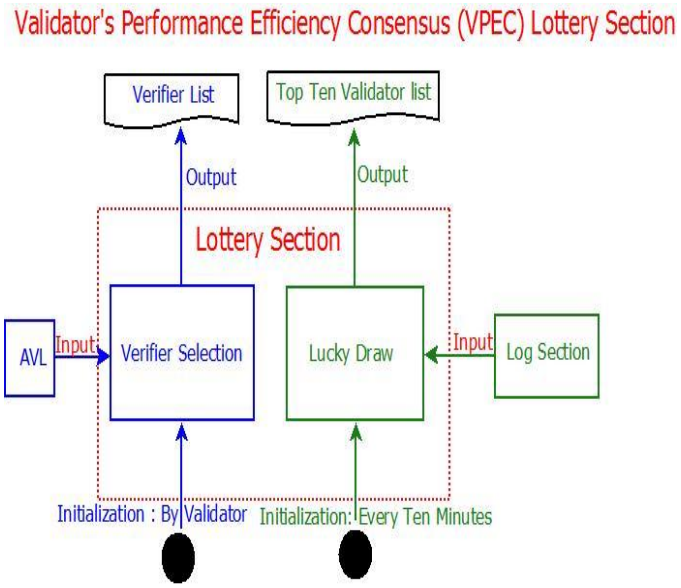

Figure 3 Overview of Lottery section of VPEC

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

4.3 VPEC Active Validators List (AVL)

Any user can be a validator in block-chain by just registering to AVL. In AVL, there are active validators and verifiers. Validators and verifiers are similar in the AVL. Their functions are different. Validators are those who receive transactions from a transaction pool. They request the lottery section to choose the verifiers from the AVL for the transaction's verification. They manage, arrange, check, and multicast transactions for verification and receive the required response from the verifiers as shown in figure 3. The Validator adds the transaction to the block and then add that valid block to the block-chain. The validators broadcast the valid block to all validators of the AVL. The lottery section does not choose validators. Validators become verifier when chosen by the lottery section from the AVL. They are receiving transactions from a transaction pool. They re-check the transaction and perform verification. If the transaction is conducted in accordance with the block-chain rules and there is no security risk in violation of the transaction, the verifier will send an "Accept" message, otherwise a "Reject" message will be sent.

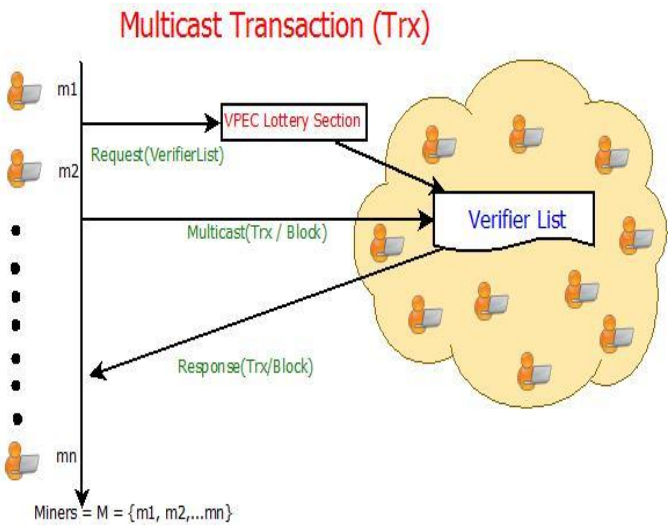

Figure 4Miner multicast transaction to verifier list

4.4 VPEC Log List Section

The VPEC Log is a history list of transactions confirmation and verification activities. It shows the number of transactions validated/verified by the validators of AVL. It is an essential list of VPEC. It is required in section 2 of the lottery section, to incentivize the validators for creating a new block for the block-chain. The log list contains the validator's PseudoID, transaction's ID, Verifier's PseudoID, timestamp and hash-code of the previous block. The hash-code of the previous block shows the location of the transaction in the block of block-chain.

4.5 VPEC Block-chain's Ledger

Block-chain's ledger is a database for storing the verified transactions in a verified block. The verified block is appended to the last block of the block-chain by a hash code. This will make the chain immutable and irreversible.

V. VPEC ANALYSIS AND EVALUATION

This section of the paper describes the theoretical evaluation and analysis; the security, forking, fairness and scalability of the proposed consensus algorithm.

5.1 Evaluation

Our consensus algorithm is based on the lucky draw mechanism. In the lucky draw, validators/verifiers are selected randomly for the validation and verification of transaction/block. In VPEC, the validators/verifiers neither do hard work such as solving a mathematical puzzle nor locking the stake in the network for a while. As a result, energy and time consumption in VPEC is reduced by a higher percentage than other consensus algorithms. Therefore, throughput will be n times higher than algorithms based on hard work and stake-holding. Most of the available consensus algorithms are based on a capitalistic approach. This is a challenge for ordinary people in the society who want to mine. Ordinary people cannot purchase very expensive advanced computing devices. They cannot even join a mining pool to share resources or stake some amount. Therefore, our approach retains fairness. It provides equal opportunities to all the validators for

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

mining. They can get rewards for creating new blocks in the block-chain network. There is no scalability issue in VPEC. The minimum number of validators/verifier must not be less than two in AVL. One will be a receiver of the transactions from the pool, and the other will be the verifier of the transactions. It shows that there are more than two validators/verifiers, which proves that VPEC is a scalable consensus algorithm. Experiments will be conducted to assess the scalability, throughput, and security of the proposed consensus algorithm.

5.2 Security Analysis

Some possible frequent security attacks related to the block-chain system are forking, Sybil attack, 51% attack, double spending, etc.

5.2.1 Forking

In VPEC, the rights of creating a new block are assigned to one validator/verifier from AVL by the lottery section. Hence, there is no competition for getting the reward of new block creation. Therefore, no forking possible in the VPEC algorithm.

5.2.2 Sybil attack

The lucky draw selects validators/verifier in the VPEC. The validators/verifiers are chosen by having high efficiency in validation and verification of transaction/block as well as keeping its place in the top ten list of the AVL. Hence, the chance of a Sybil attack is hard.

5.2.3 51% attack

In VPEC, the lottery section randomly selects 50% +1 validators/verifier from the AVL. It is hard to know about the validators/verifiers in advance. Therefore, the chance of 51% is less. The 51% attack is possible when all the validators in the AVL make collusion. If a single validator, not included in the collusion, then the chance of the 51% attack is decreasing. Because in the VPEC, the finality of a transaction or a new block creation is based on 100% positive response of the validators.

5.2.4 Double spending attack

The validators are taking transactions from the pool. The transaction pool prevents a similar transaction from the same user until the transaction is added to the block. It helps in preventing the double spending of transaction.

VI. COMPARISON OF VPEC WITH OTHER ALGORITHMS

The comparative summary of VPEC with PoW and PoS consensus algorithms are shown in the Table 2.

Table 2: VPEC Comparison with Other Consensus Algorithms

Properties	**Consensus Algorithms**		
	PoW	PoS	VPEC
Block-chain type	Public	Both	Both
Scalability	High	High	High
Throughput	low	high	High
Fault tolerance	<=25%	Byzantine fault tolerance and crush fault 50%	No chance of Byzantine fault availability
Participation cost	Yes (purchasing ASIC h.w)	Yes (stake)	No
Energy consumption	high	low	Low
Chance of Forking	yes	Yes	No
Fairness	No	No	Yes

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

6.1 Scalability

There is no scalability issue arises in the PoW, PoS, and VPEC as they have permissionless nature.

6.2 Throughput

All the algorithms shown in the Table 2 except PoW, have a high throughput in which there is no hardworking mechanism used like finding a specific number of hash value for the block which is time consuming. As we know that hardworking mechanism is inversely proportional to the throughput. If more hard work requires for finding the difficult value, the less throughput will be the result.

6.3 Fault Tolerance

The goal of fault tolerance is, to solve the problem of reaching consensus when nodes behave arbitrarily or crash due to the failure of the network. The PoW and PoS are implemented practically in which the researchers measure fault tolerance property. As it is shown in Table 2. The block-chain network uses PoW and PoS as a consensus algorithm can tolerate the fault either Byzantine or crash up to <=25%, 50% respectively, whereas VPEC is not implemented yet. VPEC is theoretically firm and having no chance of Byzantine fault because of no voting mechanism. The lottery section selects the validators and verifiers due to which the chance of Byzantine fault come to zero.

6.4 Participation Cost and Fairness

All the algorithms mentioned in Table 1, except VPEC, make it very difficult for the poor people, who wish to join the block-chain as a validator due to the cost of using expensive technology such as ASIC (PoW), and holding stake (PoS,). VPEC does not require any expensive technology, holding stake and references to join the block-chain network for getting equal opportunity. In VPEC, poor and rich are equal.

6.5 Energy Consumption

There is no exact answer for the property "energy consumption," which is low, medium, and high. As it is not easy to provide precise numbers of how much energy each implementation uses. It is due to the confounding factors such as processor efficiency and types of technology used.

6.6 Chance of Forking

The chance of forking in PoW and PoS, is due to the greedy nature of the miner for competing for the award of a new block which causes the chain to split into two. While in VPEC there is no chance of splitting the chain. The rights of creating a new block in the VPEC is assigned to one validator/verifier from AVL by the lottery section. Hence, there is no competition or struggle for getting the reward of a new block. Therefore, no forking possible in the environment having VPEC as a consensus algorithm.

VII. CONCLUSION AND FUTURE WORK

In this paper, a new consensus algorithm is proposed for public block-chain. The philosophy of VPEC is to provide fairness to ordinary people, in terms of incentivizing them for creating a new block. VPEC does not require any expensive technology to purchase like ASIC for finding a hash value, holding a stake in the network, and references to join the block-chain. In VPEC, poor and rich people are equal to join the block-chain system. The lucky draw section in the VPEC, select validators to create a new block and the reward of a new block is awarded. Theoretically, VPEC guarantees the scalability, availability, fairness, reduce energy consumption, no forking in the block-chain. The practical implementation and formal verification of the VPEC will be studied in the future.

Acknowledgement.

The authors would like to thank UniversitiKebangsaanMalalysia for supporting this

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

work financially under the UKM grants PP-FTSM-2019 and FRGS/1/2019/ICT01/UKM/01/2.

REFERENCES

[1] Asayag, A., Cohen, G., Grayevsky, I., Leshkowitz, M., Rottenstreich, O., Tamari, R., & Yakira, D. (2018). Helix: A Scalable and Fair Consensus Algorithm Resistant to Ordering Manipulation, 1–26.

[2] Baird, L. (2018). The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance, 1–28.

[3] Chohan, U. (2018). Proof-of-Stake Algorithmic Methods: A Comparative Summary. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3131897

[4] De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. *CEUR Workshop Proceedings*, *2058*, 1–11.

[5] Husnil Khatimah, P. S. N. L. A. (2019). Hedonic motivation and social influence on behavioral intention of e-money: The role of payment habit as a mediator — The National University of Malaysia. Retrieved November 15, 2019, from https://ukm.pure.elsevier.com/en/publications/hedonic-motivation-and-social-influence-on-behavioral-intention-o

[6] Jain, A., Arora, S., Shukla, Y., Patil, T. B., & Sawant-patil, S. T. (2018). Proof of stake with Casper the friendly finality gadget protocol for fair validation consensus in Ethereum. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(3), 291–298.

[7] Kamal, N., Saad, M. H. M., Kok, C. S., & Hussain, A. (2018). Towards revolutionizing stem education via IoT and blockchain technology. *International Journal of Engineering and Technology(UAE)*, *7*(4), 189–192. https://doi.org/10.14419/ijet.v7i4.11.20800

[8] King, M. (2019). A Former Bank Of England Governor Warned The 2008 Crash That Inspired Bitcoin Could Happen Again. Retrieved November 15, 2019, from https://www.forbes.com/sites/billybambrough/2019/10/27/a-former-bank-of-england-governor-warned-the-2008-crash-that-inspired-bitcoin-could-happen-again/#1fee0b8a4214

[9] Kwon, J. (2014). TenderMint : Consensus without Mining. *The-Blockchain.Com*, *6*, 1–10. Retrieved from tendermint.com/docs/tendermint.pdf

[10] Lamport, L., Reed, B. C., Junqueira, F. P., Ongaro, D., Ousterhout, J., Olson, M. a, … Cowling, J. (2014). In Search of an Understandable Consensus Algorithm. *Atc '14*, *22*(2), 305–320. https://doi.org/10.1145/1529974.1529978

[11] Li, K., Li, H., Hou, H., Li, K., & Chen, Y. (2018). Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain. *Proceedings - 2017 IEEE 19th Intl Conference on High Performance Computing and Communications, HPCC 2017, 2017 IEEE 15th Intl Conference on Smart City, SmartCity 2017 and 2017 IEEE 3rd Intl Conference on Data Science and Systems, DSS 2017*, *2018-Janua*, 466–473. https://doi.org/10.1109/HPCC-SmartCity-DSS.2017.61

[12] Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The Honey Badger of BFT protocols. *Proceedings of the ACM Conference on Computer and Communications Security*, *24-28-Octo*(Section 3), 31–42. https://doi.org/10.1145/2976749.2978399

[13] Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016). Proof of Luck: An efficient blockchain consensus protocol. *SysTEX 2016 - 1st Workshop on System Software for Trusted Execution, Colocated with ACM/IFIP/USENIX Middleware 2016*, 2–7. https://doi.org/10.1145/3007788.3007790

May – June 2020
ISSN: 0193-4120 Page No. 17530 - 17539

[14] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A Review on Consensus Algorithm of Blockchain, 2567–2572.

[15] Mizoguchi, T. J., & Lippard, S. J. (1998). Synthetic models of the deoxy and oxy forms of the non-heme dioxygen- binding protein hemerythrin [24]. *Journal of the American Chemical Society*, *120*(42), 11022–11023. https://doi.org/10.1021/ja982417z

[16] Muratov, F., Lebedev, A., Iushkevich, N., Nasrulin, B., & Takemiya, M. (2018). YAC: BFT Consensus Algorithm for Blockchain. Retrieved from http://arxiv.org/abs/1809.00554

[17] Nur Husna Azizul, Abdullah Mohd Zin, Ravie Chandren Muniyandi, Z. S. (2019). Authentication and authorization design in Honeybee computing — The National University of Malaysia. Retrieved November 15, 2019, from https://ukm.pure.elsevier.com/en/publications/authentication-and-authorization-design-in-honeybee-computing

[18] Reis, J., Amorim, M., Melao, N., & Matos, P. (2016). Digital Transformation : A Literature Review and Guidelines for Future Digital Transformation : A Literature Review and Guidelines for Future Research. *10th European Conference on Information Systems Management. Academic Conferences and Publishing Limited*, *1*(March), 20–28. https://doi.org/10.1007/978-3-319-77703-0

[19] Safavi, S., Meer, A. M., Keneth Joel Melanie, E., & Shukur, Z. (2019). Cyber Vulnerabilities on Smart Healthcare, Review and Solutions. *Proceedings of the 2018 Cyber Resilience Conference, CRC 2018*, 1–5. https://doi.org/10.1109/CR.2018.8626826

[20] Sankar, L. S., Vidyapeetham, A. V., Sindhu, M., Vidyapeetham, A. V., Sethumadhavan, M., Vidyapeetham, A. V., … Slice, Q. (2017). Survey of Consensus Protocols on Blockchain Applications.

[21] Satoshi, N. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3440802

[22] Schwartz, D., Youngs, N., & Britto, A. (2014). The Ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, 1–8. Retrieved from http://www.naation.com/ripple-consensus-whitepaper.pdf

[23] Siew Pheng Chan, William C. Chui, Kwok Wing Lro, Kuo Chin Huang, Normita D. Leyesa, Wen Yuan Lin, Roberto C. Mirasol, Yolanda R. Robles, Beng Hea Tey, T. P. (2012). Consensus statement: Appropriate consumer education and communication programs for weight- loss agents in Asia — The National University of Malaysia. Retrieved November 15, 2019, from https://ukm.pure.elsevier.com/en/publications/consensus-statement-appropriate-consumer-education-and-communicat

[24] Snider, M., Samani, K., & Jain, T. (2018). Delegated Proof of Stake: Features and Tradeoffs. *Multicoin Capital*, 19. Retrieved from https://multicoin.capital/2018/03/02/delegated-proof-stake-features-tradeoffs/

[25] Xue, T., Yuan, Y., Ahmed, Z., Moniz, K., Cao, G., & Wang, C. (2018). Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency. *Proceedings - International Computer Software and Applications Conference*, *1*, 636–644. https://doi.org/10.1109/COMPSAC.2018.00096

[26] Yli-huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology ?— A Systematic Review, 1–27. https://doi.org/10.1371/journal.pone.0163477